



OCSP Monitor

Service status checking and reporting



ascertia

Online Certificate Status Protocol (OCSP) servers are the cornerstone of a trusted PKI infrastructure, providing essential e-ID validation services and are the basis for checking the trust and managing the liability associated with this. It is crucial that they are correctly configured, remain highly available to relying parties and that they are regularly checked for correct operation. Knowing what service level has been attained is key to capacity planning and an effective reporting tool is an essential part of this. OCSP Monitor delivers all this.

Automated OCSP Monitoring

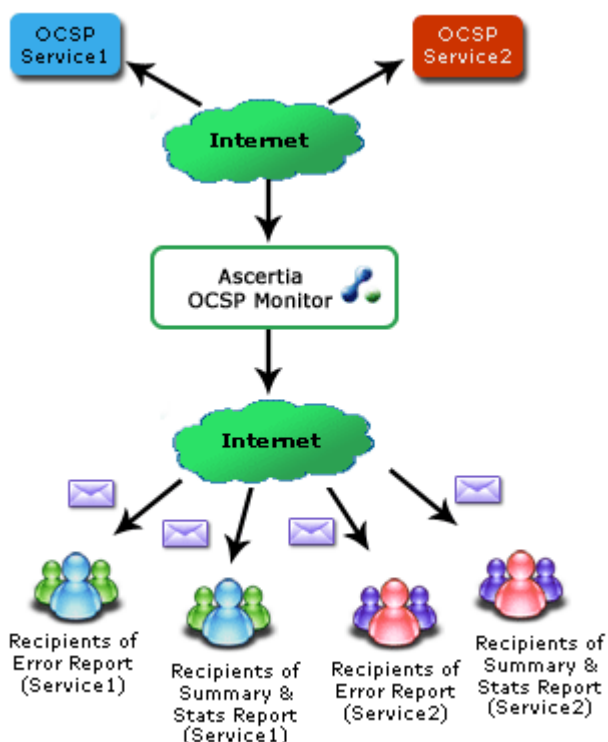
Ascertia OCSP Monitor is a sophisticated test product that enables security administrators to easily detect OCSP service failures or irregularities. It is designed for 24 x 7 automated monitoring although it can also be used interactively when required. OCSP Monitor enables administrators to identify availability or security policy issues and fix unexpected conditions before users report them.

OCSP Monitor is also very useful for organisations that consume OCSP services. They can monitor the service and easily compare this with the Service Level Agreement (SLA). An end-of-day report provides all the key statistics required.

Maximise your OCSP Server uptime

OCSP Monitor provides immediate real-time feedback on OCSP validation issues as they arise. Where OCSP services are used it is often assumed that they are functioning correctly and will continue to do so - this is often not the case.

OCSP Monitor allows multiple test scenarios to be run. These can check for expected and unexpected behaviours and monitor OCSP server performance.



Why use OCSP Monitor

- ➔ Monitor one or more OCSP services for correct functioning, unexpected results, availability and performance - automatically and continuously
- ➔ Use simple tests to check for Responder availability and obtain summary SLA data
- ➔ Use multiple tests within a test scenario to check compliance with expected validation policy settings and review any detailed error reports and end of day test summary reports
- ➔ Select which admin staff receive error reports and summary reports by email and/ or SMS
- ➔ Test all accessible responders (primary, back-up, test) from a single location with a single tool
- ➔ OCSP Monitor is an RFC 2560 compliant OCSP client and can communicate with any compliant responder
- ➔ Easy to deploy and use - no server-side component or agent is required for monitoring

Perform real-time tests

OCSP Monitor tests the actual status of your OCSP Responder by making real OCSP client requests. This is the only way to measure the server response times seen by end-users.

OCSP Monitor is extremely easy to set up and use so that multiple test scenarios, each with one or more test cases can be monitored. These are easy to change as required.

The following screen shows the live report dashboard screen that allows administrators to review the results obtained from test scenarios run since midnight.

Test Scenario & Cases	Start	Stop	Freq. (Min.)	18:10	18:12	18:14	18:16	18:18	18:20	18:22	18:24	18:26	18:28	18:30	18:32	18:34	18:36	18:38	18:40	18:42	18:44	18:46	18:48	18:50	18:52
OCSP Test Scenario1	01:00	23:50	2																						
Check Revocation Status1				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Check Revocation Status2				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
OCSP Test Scenario2	01:02	23:02	2																						
Check Revocation Status1				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Check Revocation Status2				●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Continuous Monitoring

OCSP Monitor runs continuously and can allow various Test Scenarios to be run to monitor performance and validation policy. Ascertia recommends:

- ➔ Checking availability and response times by running a simple check on a valid certificate once every few minutes
- ➔ Checking that a fresh CRL is being used by the OCSP responder – using a CRL freshness policy test run as required, e.g. every hour
- ➔ Running a comprehensive policy check twice a day to ensure that the defined validation policy is being enforced, e.g. correct trusted, not trusted results issued, valid OCSP signatures, checking nonce and unauthorised request handling
- ➔ Running checks on disaster recovery systems to ensure they are operational

Detailed Monitoring Checks and Alerts

OCSP Monitor has been designed by security experts to provide high quality management information, for example:

- ➔ Each test scenario can have several test cases to perform multiple positive and negative checks
- ➔ Each test scenario can have its own trust anchors defined for accurate trust checking
- ➔ When a test scenario fails a customisable failure report is sent to a defined list of operations staff - each scenario can have different staff identified
- ➔ Customisable reports can be sent using SMS or email or both as required - both internal and external staff can be notified - useful when using managed services
- ➔ When a scenario completes a summary report can be sent to selected service management staff showing the minimum, average and maximum response delay statistics observed as well as a summary of the successful and failed tests observed during the period
- ➔ At the end of day a summary report for all scenarios can be sent to service management staff detailing the main statistics for all scenarios

System Support

OCSP Monitor currently supports Windows systems only.

System Requirements:	Windows 2003, Windows 2000, Windows XP
Interfaces and Protocols:	RFC 2560 (OCSP), TLS/SSL, Communication through proxy (including digest authentication) PFX/PKCS#12 for OCSP request signing, X.509v1 and v3 certificates.

Easy Configuration

OCSP Monitor has an intuitive wizard to help set-up test scenarios and the required test cases within these. Each test scenario can be set to run between specific start and stop times. Reports can be customised per test scenario as shown below:



Clear Reporting

OCSP Service Level Agreements can now be accurately checked and reported on. The identification and reporting of OCSP service issues identification has always been rather hit and miss until now. OCSP Monitor provides for easy change of test policies so that a selected level of detailed testing can be carried as required to suit the business demands. History data is maintained and detailed English language analysis of OCSP request and response data is available as a standard feature.

A typical summary report email is shown below which details the key statistics and the highlighted unexpected failures that were detected:

Subject: Your test case scenario has completed for today



Please review below the statistics of your test case scenario. Further details including the actual OCSP request / response transactions can be viewed from the OCSP Monitor History Viewer.

Scenario Summary Report

Scenario Name:	Daily Test Scenario for OCSP Responder Service
Scenario Start Time:	16:30:16
Scenario Stop Time:	17:30:16
Number of times scenario was run:	6
Time Interval:	10 mins
OCSP Responder:	http://ocsp.globaltrustfinder.com:80

Summary Report Created At:	Friday, July 07, 2006 17:30:53
Minimum Response Time:	1.12 (sec)
Average Response Time:	1.23 (sec)
Maximum Response Time:	1.37 (sec)
Total Test Cases Failed:	6
Total Test Cases Passed:	12

Test Case Name	Number of Failures
Test case 1 - testing of a good certificate	0
Test case 2 - Testing of a revoked certificate	0
Test case 3 - Deliberate test case which should fail	6

Ascertia Limited
 Web: www.ascertia.com
 Email: info@ascertia.com
 Tel: +44 1256 895416 US: +1 508 283 1890
 40 Occam Road, Guildford, Surrey, GU2 7YG, UK
 © Copyright Ascertia Limited 2009. All Rights Reserved